AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Previously presented) A method for establishing a secure communication channel in an IP telephony network between a first and a second user, wherein the first user and the second user are coupled to first and second telephony adapters, which in turn, are coupled to first and second gateway controllers, respectively, wherein the gateway controllers control user access to the IP telephony network, and wherein the telephony adapters encrypt and decrypt user information exchanged over the IP telephony network, the method comprising:

receiving a request at the first gateway controller to establish a secure communication channel between the first user and the second user;

generating a secret key at the first gateway controller;

distributing the secret key to the first and second telephony adapters over previously established secure connections; and

establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key,

wherein call signaling messages between the first telephony adapter and the second telephony adapter are routed through the first gateway controller and the second gateway controller, and encrypted messages are exchanged between the first telephony adapter and the second telephony adapter on the secure communication channel.

2. (Original) The method of claim 1 wherein the step of generating comprises a step of generating a random number at the first gateway controller to be used as the secret key.

3. (Original) The method of claim 1 wherein the step of generating comprises a step of deriving the secret key at the first gateway controller, wherein the secret key is derived from a signaling key shared between the first telephony adapter and the first gateway controller.

4. (Original) The method of claim 1 wherein the step of distributing comprises steps of:

transmitting the secret key from the first gateway controller to the second gateway controller;

transmitting the secret key from the second gateway controller to the second telephony adapter

transmitting the secret key from the first gateway controller to the first telephony adapter.

5. (Original) The method of claim 1 further comprising steps of;

receiving a request at the first gateway controller to provide the secret key to a law enforcement server; and

providing the secret key to the law enforcement server.

6. (Previously presented) An IP telephony network for establishing a secure communication channel between a first user and a second user, wherein the first user and the second user are coupled to first and second telephony adapters, which in turn, are coupled to first and second gateway controllers, respectively, wherein the gateway controllers control user access to an IP telephony backbone, and wherein the telephony adapters encrypt and decrypt user information exchanged over the IP telephony network, the IP telephony network comprising:

means for receiving a request at the first gateway controller to establish a secure communication channel between the first user and the second user;

means for generating a secret key at the first gateway controller;

means for distributing the secret key to the first and second telephony adapters over a previously established secure connection; and

means for establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key,

wherein call signaling messages between the first telephony adapter and the second telephony adapter are routed through the first gateway controller and the second

gateway controller, and encrypted messages are exchanged between the first telephony adapter and the second telephony adapter on the secure communication channel.

7. (Previously presented) A gateway controller for establishing a secure communication channel in an IP telephony network, the gateway controller coupled between a telephony adapter and a telephony network backbone, the gateway controller comprising:

a key creation module having logic to create a secret key;

a key storage module coupled to the key creation module and having logic to store the secret key; and

a message processor coupled to the key creation module and the key storage module, and having logic to process messages exchanged between the telephony adapter and the telephony network backbone, wherein the message processor further comprises:

logic to receive a request to establish a secure communication channel between a first user and a second user, the first user couple to the telephony adapter, the second user coupled to a remote telephony adapter;

logic to distributed the secret key to the telephony adapters over previously established secure connections, whereby the secure communication channel between the first user and the second user may be established by encrypting and decrypting information using the secret key,

wherein call signaling messages between the first telephony adapter and the second telephony adapter are routed through the first gateway controller and the second gateway controller, and encrypted messages are exchanged between the first telephony adapter and the second telephony adapter on the secure communication channel.

8. (Original) The gateway controller of claim 7 wherein the key creation module has logic to generate a random number as the secret key.

9. (Original) The gateway controller of claim 7 wherein the key creation module has logic to derive the secret key from a signaling key shared with the telephony adapter.

10. (Original) The gateway controller of claim 7 wherein the key storage module has logic to encrypt the secret key before storage, using a public/private key pair belonging to law enforcement.

11. (Previously presented) A system for providing encrypted communications in an IP telephony network, said system comprising:

a first cable telephony adapter;

a first gateway controller coupled with said first cable telephony adapter;

a second cable telephony adapter;

a second gateway controller coupled with said second cable telephony adapter;

a network coupled with both said first gateway controller and said second gateway controller so as to facilitate communications between said first cable telephony adapter and said second cable telephony adapter, wherein said communications comprise call signaling messages between said first cable telephony adapter and said second cable telephony adapter that are routed through said first gateway controller and said second gateway controller, and said communications further comprise encrypted communications that are exchanged between said first cable telephony adapter and said second cable telephony adapter;

wherein said first gateway controller comprises:

a first key creation module configured to generate a secret key for distribution to both said first cable telephony adapter and said second cable telephony adapter for use in encrypted communications between said first cable telephony adapter and said second cable telephony adapter.

12. (Previously presented) The system as described in claim 11 wherein said second gateway controller comprises:

a second key creation module configured to generate a secret key for distribution to both said first cable telephony adapter and said second cable telephony adapter for use

in encrypted communications between said first cable telephony adapter and said second cable telephony adapter.

13. (Previously presented) The system as described in claim 11 wherein said first gateway controller further comprises:

a message processor configured to receive an encrypted message from said first cable telephony adapter intended for decryption by said second cable telephony adapter and further configured to forward said encrypted message to said second gateway controller without decrypting said encrypted message.

14. (Previously presented) The system as described in claim 11 wherein said key creation module is configured to intermittently generate a second secret key and to distribute said second secret key to said first cable telephony adapter and said second cable telephony adapter so as to replace said previously generated secret key.

15. (Previously presented) A method of establishing secure communications between a first cable telephony adapter and a second cable telephony adapter in a system in which secure communications do not previously exist between said first cable telephony adapter and said second cable telephony adapter, wherein said first cable telephony adapter is coupled with a first gateway controller, said second cable telephony adapter is coupled with a second gateway controller, and a network is coupled with said first gateway controller and said second gateway controller, said method comprising:

receiving at said first gateway controller a request from said first cable telephony adapter to establish communications between said first cable telephony adapter and said second cable telephony adapter;

generating a secret key at said first gateway controller;

distributing said secret key to said second gateway controller via a secure communication;

distributing said secret key from said second gateway controller to said second cable telephony adapter;

distributing said secret key from said first gateway controller to said first cable telephony adapter,

wherein call signaling messages between the first telephony adapter and the second telephony adapter are routed through the first gateway controller and the second gateway controller, and encrypted messages are exchanged between the first telephony adapter and the second telephony adapter on the secure communication channel.

16. (Previously presented) The method as described in claim 15 and further comprising:

encrypting a message at said first cable telephony adapter with said secret key;

sending said encrypted message to said first gateway controller;

receiving said encrypted message at said first gateway controller;

forwarding said encrypted message from said first gateway controller to said second gateway controller without decrypting said encrypted message.

17. (Previously presented) The method as described in claim 16 and further comprising:

receiving said encrypted message at said second gateway controller;

forwarding said encrypted message from said second gateway controller to said second cable telephony adapter without decrypting said message;

decrypting said encrypted message at said second cable telephony adapter.

18. (Previously presented) The method as described in claim 15 and further comprising:

encrypting a message at said first cable telephony adapter with said secret key;

sending said encrypted message to said first gateway controller;

receiving said encrypted message at said first gateway controller;

routing said encrypted message from said first gateway controller to said second cable telephony adapter.

19. (Previously presented) The method as described in claim 15 and further comprising:

receiving said encrypted message at said second cable telephony adapter;

decrypting said encrypted message at said second cable telephony adapter with said secret key.